

INFORMACJA O ZAGROŻENIACH

dla bezpieczeństwa i zdrowia występujących podczas pracy na terenie jednostek organizacyjnych Izby Administracji Skarbowej w Katowicach

Podczas przebywania i wykonywania prac na terenie jednostek organizacyjnych Izby Administracji Skarbowej w Katowicach objętych umową, osoby zatrudnione u innego pracodawcy powinny zwrócić szczególną uwagę na zagrożenia, z którymi mogą się spotkać, m.in. w sytuacjach:

- 1) przemieszczania się na terenie obiektów (ciągi komunikacyjne wewnątrz i na zewnątrz budynków, parkingi, place manewrowe, rampy rozładunkowe itp.), możliwość poślizgnięcia, potknięcia, upadku z wysokości, potrącenia przez poruszające się środki transportu;
- 2) korzystania z dźwigów osobowych szczególnie podczas wsiadania lub wysiadania – m.in. możliwość upadku z wysokości;
- 3) korzystania z maszyn, urządzeń i narzędzi – możliwość doznania urazu w wyniku używania niesprawnego lub uszkodzonego sprzętu;
- 4) kontaktu z uszkodzonymi przewodami, przełącznikami, gniaздkami itp. – możliwość porażenia prądem elektrycznym;
- 5) wykonywania pracy na wysokości – możliwość upadku, doznania urazu np. z powodu używania niesprawnego sprzętu, nieużywania lub nieprawidłowego używania przez pracowników środków ochrony indywidualnej;
- 6) pożaru – możliwość poparzenia, zatrucia.

Działania ochronne i zapobiegawcze, które winny być podjęte w celu wyeliminowania lub ograniczenia ww. zagrożeń:

- 1) przestrzeganie przepisów bezpieczeństwa i higieny pracy oraz przepisów przeciwpożarowych;
- 2) stosowanie środków ochrony indywidualnej oraz odzieży i obuwia roboczego;
- 3) korzystanie z maszyn, urządzeń i narzędzi tylko przez osoby do tego upoważnione, posiadające odpowiednie uprawnienia i kwalifikacje;
- 4) zakaz spożywania na terenie Urzędu napojów alkoholowych, narkotyków i innych środków odurzających;
- 5) zakaz wchodzenia i przebywania na terenie Urzędu po spożyciu napojów alkoholowych, narkotyków i innych środków odurzających;
- 6) zakaz palenia wyrobów tytoniowych – także e-papierosów we wszystkich obiektach zakładu pracy. Palenie wyrobów tytoniowych w obrębie budynku dopuszczalne jest wyłącznie w odpowiednio zorganizowanych palarniach lub na zewnątrz budynku;
- 7) zakaz używania otwartego ognia;
- 8) poinformowanie osób zatrudnionych u innego pracodawcy o osobach wyznaczonych do udzielania pierwszej pomocy oraz lokalizacji apteczek na terenie danego obiektu;
- 9) zapoznanie osób zatrudnionych u innego pracodawcy z Instrukcją bezpieczeństwa pożarowego danego obiektu oraz przekazanie informacji o pracownikach wyznaczonych do wykonywania działań w zakresie zwalczania pożarów i ewakuacji pracowników;

10) każde zauważone zagrożenie, incydent lub wypadek należy zgłosić koordynatorowi sprawującemu nadzór nad bezpieczeństwem i higieną pracy.

TELEFONY ALARMOWE

Pogotowie ratunkowe 999

Straż Pożarna 998

Policja 997

Uwaga:

Uzyskanie powyższych informacji potwierdza się podpisem w „WYKAZIE OSÓB”, stanowiącym Załącznik nr 4 do Umowy.

WYKAZ OSÓB

wykonujących pracę na terenie jednostek organizacyjnych Izby Administracji Skarbowej w Katowicach,
będących pracownikami innego pracodawcy, którzy zostali poinformowani o zagrożeniach dla bezpieczeństwa i zdrowia

Zostałem/am poinformowany/a o zagrożeniach dla bezpieczeństwa i zdrowia występujących na terenie jednostek organizacyjnych Izby Administracji Skarbowej w Katowicach objętych Umową Nr XX/2026, co potwierdzam podpisem:

Lp.	Nazwa i adres pracodawcy	Imię i nazwisko pracownika	Data i czytelny podpis pracownika	Imię i nazwisko oraz podpis informującego o zagrożeniach	Uwagi
1.	2.	3.	4.	5.	6.

Podstawa prawna:

§ 2 ust. 2 rozporządzenia Ministra Gospodarki i Pracy z dnia 27 lipca 2004 roku w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy (Dz.U. Nr 180, poz. 1860 z późn. zm.)

.....
(miejscowość i data)¹

.....
(Nazwisko i Imię)

.....
(Nazwa podmiotu zewnętrznego realizującego
usługi na rzecz Resortu Finansów)

.....
(Stanowisko/funkcja)

OŚWIADCZENIE
o zapoznaniu się z zasadami bezpieczeństwa informacji w Resorcie Finansów
we współpracy z podmiotami zewnętrznymi

W związku z realizacją zobowiązań z tytułu Umowy/Porozumienia² Nr..... z dnia
oświadczam, że zapoznałam/em się z *Zasadami bezpieczeństwa informacji w Resorcie Finansów we*
współpracy z podmiotami zewnętrznymi, stanowiącymi załącznik do niniejszego oświadczenia.

.....
(czytelny podpis)³

¹ wypełnić tylko w wersji papierowej

² niewłaściwe skreślić

³ wypełnić tylko w wersji papierowej

Zasady bezpieczeństwa informacji w Resorcie Finansów we współpracy z podmiotami zewnętrznymi

1. W Resorcie Finansów w ramach współpracy z podmiotami zewnętrznymi stosuje się następujące zasady dotyczące bezpieczeństwa informacji:
 - 1) zasada wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań (różne zadania oznaczają różną wiedzę konieczną do ich wykonania, a tym samym inny profil dostępu);
 - 2) zasada potrzeby koniecznej - pracownicy mają zapewniony dostęp tylko do środków przetwarzania informacji (urządzeń teleinformatycznych, systemów, aplikacji, pomieszczeń), które są im konieczne do wykonania powierzonych im zadań;
 - 3) zasada uprawnionego dostępu – pracownicy są dopuszczeni do przetwarzania informacji prawnie chronionych i przeznaczonych wyłącznie do użytku wewnętrznego po uzyskaniu wiedzy z zasad postępowania, w tym ochrony, określonych grup informacji; oraz do odbycia szkolenia z zasad ochrony informacji (w celu spełnienia kryteria dopuszczenia do przetwarzania określonych informacji i danych);
 - 4) zasada obecności koniecznej – prawo przebywania w obszarze przetwarzania, w tym przechowywania informacji i danych prawnie chronionych i wrażliwych, mogą mieć tylko osoby upoważnione. Przebywanie osób nieupoważnionych w tym obszarze jest możliwe wyłącznie w obecności upoważnionych pracowników;
 - 5) zasada świadomości zbiorowej - wszyscy pracownicy mają świadomość konieczności ochrony aktywów informacyjnych i aktywnie uczestniczą w tym procesie; świadomość pracowników w zakresie istniejących zagrożeń i zasad ochrony informacji jest podnoszona, w szczególności przez szkolenia i działania informacyjne;
 - 6) indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych na nich obowiązków i nadanych im uprawnień. Zasada ta dotyczy np. powierzonego sprzętu:
 - każdy pracownik odpowiada za powierzony mu do użytkowania sprzęt komputerowy, wydruków z systemu centralnego wydruku,
 - każdy pracownik odpowiada za sporządzony przez siebie wydruk;
 - 7) rozdzielania obowiązków - zadania krytyczne z punktu widzenia bezpieczeństwa systemu nie mogą być realizowane przez jedną osobę. Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić w celu ograniczenia okazji do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia aktywów organizacji, w szczególności należy rozdzielić realizację funkcji operacyjnych od nadzorczych i kontrolnych;
 - 8) czystego biurka - podczas nieobecności pracownika na stanowisku pracy, także w przypadku krótkotrwałego opuszczenia pomieszczenia, dokumenty i informatyczne nośniki danych zawierające informacje prawnie chronione lub przeznaczone wyłącznie do użytku wewnętrznego należy zabezpieczyć przed dostępem osób postronnych i nieupoważnionych. Środki organizacyjno-techniczne dot. przechowywania dokumentów i informatycznych nośników danych dostosowywane są zidentyfikowanego ryzyka, z wykorzystaniem m.in. nieprzeszlonych, zamykanych na klucz mebli biurowych, szaf metalowych zamykanych na klucz lub kod, przeznaczonych do tego pomieszczeń zamykanych na klucz lub wyposażonych w system kontroli dostępu;

- 9) czystego ekranu - na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym – w szczególności dotyczy to serwera obsługującego systemy alarmowe, komputerów administratorów, serwerów do monitoringu. W czasie obecności pracownika monitor jest ustawiony tak, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;
- 10) czystego kosza – dokumenty papierowe, z wyjątkiem materiałów zawierających informacje publicznie dostępne, w tym promocyjno-informacyjne, muszą być niszczone w sposób uniemożliwiający ich odczytanie lub odtworzenie. W celu zniszczenia dokumentów papierowych zawierających informacje prawnie chronione i przeznaczone wyłącznie do użytku wewnętrznego należy korzystać z udostępnionych niszczarek o odpowiedniej klasie niszczenia, adekwatnej do informacji oraz danych utrwalonych na niszczonych dokumentach. Niszczenie informatycznych nośników danych należy przeprowadzić zgodnie z zasadami określonymi w umowie/porozumieniu;
- 11) czystej tablicy - po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice oraz flipchart (tablice do szkoleń);
- 12) czystych drukarek – w przypadku drukowania dokumentów z użyciem ogólnodostępnej drukarki drukowane informacje są zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik ma obowiązek skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru;
- 13) poufności informacji uwierzytelniających – każdy pracownik jest obowiązany do zachowania poufności udostępnionych mu haseł, kodów dostępu, kodów PIN, w szczególności do systemów informacyjnych;
- 14) prywatności kont w systemach – każdy użytkownik jest obowiązany do pracy w systemach informacyjnych wyłącznie na przypisanych lub udostępnionych mu kontach, które jednoznacznie go identyfikują. Zabronione jest udostępnianie własnych kont osobom trzecim. Zasada ta ma również zastosowanie do kart wykorzystywanych w systemach kontroli dostępu funkcjonujących w Resorcie Finansów. Stosowanie się do tej reguły pozwala zachować rozliczalność działań użytkowników;
- 15) dyskrekcji – wszelkie informacje służbowe mogą być przekazywane innym osobom uprawnionym do pozyskania tych informacji zgodnie z obowiązującymi przepisami prawa i przyjętymi w Resorcie Finansów zasadami;
- 16) zamkniętego pomieszczenia – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu. Na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest obowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;
- 17) zgłaszania incydentów bezpieczeństwa informacji i naruszeń ochrony danych osobowych – każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu lub naruszenia mającego lub mogącego mieć wpływ na bezpieczeństwo informacji, w tym danych osobowych w Resorcie Finansów;
- 18) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę, w tym umowy, porozumienia, zawierają stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu aktywów informacyjnych po zakończeniu współpracy;
- 19) automatyzacji backupu - procesy tworzenia kopii zapasowych są odpowiednio zaplanowane z uwzględnieniem wymogów prawnych i potrzeb Resortu Finansów, jak również są zautomatyzowane oraz niemożliwe do przerwania przez pracownika;

- 20)** legalnego oprogramowania – na serwerach i stacjach roboczych jest zainstalowane wyłącznie legalne oprogramowanie;
 - 21)** ochrony zewnętrznych (wymennych) nośników danych – dane i informacje utrwalone na zewnętrznych nośnikach danych i wynoszone poza pomieszczenia użytkowane przez Resort Finansów są odpowiednio zabezpieczone przed nieuprawnionym dostępem, zniszczeniem oraz utratą integralności w czasie transportu i przechowywania. W szczególności dotyczy to informacji prawnie chronionych np. tajemnicy skarbowej, tajemnicy celnej, danych osobowych.
 - 22)** zasada bezpieczeństwa informacji w usługach chmurowych - wszystkie dane przetwarzane w usługach chmurowych muszą być lokalizowane w regionach Europejskiego Obszaru Gospodarczego (EOG), z preferencją regionów zlokalizowanych w Polsce. Odstępstwa od tej zasady wymagają uprzedniej zgody DBE MF, opartej na analizie ryzyka wraz z zastosowaniem mechanizmów transferowych i technicznych środków ochrony (np. szyfrowanie, kontrola kluczy). W przypadku, gdy przetwarzanie obejmuje dane osobowe, odstępstwa od lokalizacji EOG wymagają również oceny zgodności transferu danych zgodnie z RODO oraz zastosowania adekwatnych mechanizmów transferowych i środków technicznych.
- 2. Stosowanie zabezpieczeń lub ich grup uwzględnia następujące zasady:**
- 1)** minimalny stosowany poziom zabezpieczeń odpowiada wymogom obowiązujących przepisów prawa;
 - 2)** zabezpieczenia są wdrażane we wszystkich obszarach określonych w deklaracji stosowania zabezpieczeń, zgodnie z wymogami normy ISO/IEC 27001 i zasadami określonymi w normie ISO/IEC 27002;
 - 3)** używane mechanizmy zabezpieczeń są adekwatne (odpowiednie) do zagrożeń, podatności, wartości aktywów oraz wyników szacowania ryzyka w bezpieczeństwie informacji;
 - 4)** w doborze zabezpieczeń należy uwzględnić zalecenia i rekomendacje sformułowane w wyniku przeprowadzonych audytów bezpieczeństwa i kontroli;
 - 5)** zabezpieczenia fizyczne, techniczne, prawne i organizacyjne uzupełniają się wzajemnie (grupy zabezpieczeń), zapewniając wymagany poziom bezpieczeństwa informacji;
 - 6)** należy unikać niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych Resortu Finansów;
 - 7)** niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających systemy informacyjne funkcjonujące w Resorcie Finansów bez zastosowania alternatywnych mechanizmów; systemy są sprawne i przygotowane na wystąpienie zidentyfikowanych zagrożeń;
 - 8)** domniemanej odmowy - przyjęcia jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach („to, co nie jest dozwolone, jest zabronione”);
 - 9)** ciągłego doskonalenia – SZBI jest stale monitorowany, stosowane zabezpieczenia są dostosowywane do zmieniających się warunków wewnętrznych i zewnętrznych, w celu zapewnienia ich przydatności, adekwatności i skuteczności.